UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/775,804	02/09/2004	Steven T. Kirsch	PRO-012	9685

3897 7590 08/06/2008

SCHNECK & SCHNECK
P.O. BOX 2-E
SAN JOSE, CA 95109-0005

EXAMINER	
AVERY, JEREMIAH L	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
08/06/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/775,804	KIRSCH, STEVEN T.	
	Examiner	Art Unit	
	JEREMIAH AVERY	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 May 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-38 have been examined.

2. Responses to Applicant's remarks have been given.

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 5/19/08 has been entered.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-33, 35-37 and 39-47 are rejected under 35 U.S.C. 102(e) as being anticipated by United States Patent Application Publication No. 2006/0265689 to Kuznetsov et al., hereinafter Kuznetsov.

1. Regarding claim 1, Kuznetsov teaches a method for accelerating delivery of requested secure webpages comprising:

rewriting, with a client proxy, original format links in first webpages identifying secure webpages so that any request for a secure webpage made by referencing a rewritten link will be recognized by an intermediating device intermediating between a client and a server capable of responding to the request for the secure webpage (page 4, paragraph 27, "URL re-writing" and page 11, paragraphs 96-99, "rewriting URLs in an HTTP header" and "transformation of pre-transform data according to a transformation function");

receiving a request, for the secure webpage, made using a rewritten link in a received webpage (page 3, paragraph 25, paragraph 27, "URL re-writing", page 6, paragraphs 56 and 57, page 7 and paragraph 63 page 4, and page 11, paragraphs 96-99, "rewriting URLs in an HTTP header" and "transformation of pre-transform data according to a transformation function");

returning the rewritten link to its original format to thereby accelerate delivery of the requested secure webpage (page 12, paragraph 128)

requesting the secure webpage from the server (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.");

receiving the requested secure webpage from the server (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web

page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.").

2. Regarding claim 2, Kuznetsov teaches the client proxy scanning the received webpage for any link to a secure webpage (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.", page 4, paragraph 27 and page 7, paragraph 60, "the markup processor 125 can operate as a security processor to handle security related processing operations on markup language data within messages 140 transferred from the client application 135 to the server application 115").

3. Regarding claims 3 and 17, Kuznetsov teaches establishing a secure connection between the intermediating device and the server responding to the request for the secure webpage (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.", page 4, paragraph 27 and page 7, paragraph 60, "the markup processor 125 can operate as a security processor to handle security related processing operations on markup language data within messages 140 transferred from the client application 135 to the server application 115").

4. Regarding claims 4 and 15, Kuznetsov teaches wherein an https link in the received webpage is rewritten to be an http link (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.", page 4, paragraph 27, "URL re-writing", page 9, paragraphs 83 and 84 and page 11, paragraphs 96-99, "rewriting URLs in an HTTP header" and "transformation of pre-transform data according to a transformation function").

5. Regarding claims 5 and 16, Kuznetsov teaches wherein an https link in the received webpage is rewritten to include a reference to a subdomain recognized by the intermediating device as indicating a request for a secure webpage (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.", page 4, paragraph 27, "URL re-writing", page 9, paragraphs 83 and 84 and page 11, paragraphs 96-99, "rewriting URLs in an HTTP header" and "transformation of pre-transform data according to a transformation function").

6. Regarding claim 6, Kuznetsov teaches establishing a secure connection between the client and the intermediating device when the request for the secure webpage is received at the device (page 1, paragraph 11, "A web server software application

operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser." and page 7, paragraph 60, "the markup processor 125 can operate as a security processor to handle security related processing operations on markup language data within messages 140 transferred from the client application 135 to the server application 115").

7. Regarding claim 7, Kuznetsov teaches returning any received webpage to the client proxy (page 3, paragraph 25, page 6, paragraphs 56 and 57, page 7 and paragraph 63).

8. Regarding claim 8, Kuznetsov teaches comprising returning any received webpage to the client (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser." and page 7, paragraph 60, "the markup processor 125 can operate as a security processor to handle security related processing operations on markup language data within messages 140 transferred from the client application 135 to the server application 115").

9. Regarding claims 9, 19 and 36, Kuznetsov teaches decrypting the secure webpage (page 2, paragraphs 16 and 18, page 3, paragraphs 21 and 23, page 4, paragraphs 30 and 34, page 10, paragraphs 93 and 94, page 11, remainder of

paragraph 94 and paragraphs 99 and 101, page 12, paragraphs 128 and 129, page 13, paragraph 133 and page 14, paragraphs 141 and 142).

10. Regarding claims 10, 20 and 37, Kuznetsov teaches compressing the secure webpage (page 4, paragraph 32).

11. Regarding claims 11 and 23, Kuznetsov teaches wherein compressing the secure webpage includes:

compressing data with encoder software running on an encoder communicating via a network with other devices, the compressed data to be transmitted to a decoder in the network running decoder software, the compressing consisting of representing runs of data with at least one identifier (page 1, paragraph 13, page 2, remainder of paragraph 13 and paragraphs 14-18, page 3, remainder of paragraph 20 and paragraphs 21 and 23, "digital signing, digital signature verification", page 6, paragraphs 57 and 58, page 7, remainder of paragraph 58 and paragraphs 60 and 63 and page 9, paragraph 82);

storing the at least one identifier and corresponding data represented by the at least one identifier in a database associated with the encoder (page 9, paragraph 78, "The rule processor 174 can consult the rule set database 128 to identify appropriate rules (i.e., to select a rule set) that match the tagged data portions 141, 142.", paragraphs 82-84, "domain identification" and paragraphs 85 and 86, page 10, paragraphs 91 and 94 and page 12, paragraphs 113-115);

transmitting from the encoder to the decoder data corresponding to the at least one identifier when the data is specifically requested by the decoder or when the encoder has no record of the at least one identifier being sent to the decoder (page 1, paragraph

13, page 9, paragraph 78, "The rule processor 174 can consult the rule set database 128 to identify appropriate rules (i.e., to select a rule set) that match the tagged data portions 141, 142.", paragraphs 82-84, "domain identification" and paragraphs 85 and 86, page 10, paragraphs 91 and 94 and page 12, paragraphs 113-115).

12. Regarding claims 12 and 24, Kuznetsov teaches wherein runs of data are represented with a single identifier (page 9, paragraph 78, "The rule processor 174 can consult the rule set database 128 to identify appropriate rules (i.e., to select a rule set) that match the tagged data portions 141, 142.", paragraphs 82-84, "domain identification" and paragraphs 85 and 86, page 10, paragraphs 91 and 94 and page 12, paragraphs 113-115).

13. Regarding claims 13 and 25, Kuznetsov teaches including transmitting from the encoder to the decoder only data required to complete a response to the request when the data has not been cached at a second database associated with the decoder (page 1, paragraph 13, page 9, paragraph 78, "The rule processor 174 can consult the rule set database 128 to identify appropriate rules (i.e., to select a rule set) that match the tagged data portions 141, 142.", paragraphs 82-84, "domain identification" and paragraphs 85 and 86, page 10, paragraphs 91 and 94 and page 12, paragraphs 113-115).

14. Regarding claim 14, Kuznetsov teaches a method for accelerating delivery of requested secure webpages comprising:

scanning a webpage to determine whether it contains any links to secure webpages (page 1, paragraph 11, "A web server software application operating in the web server

computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser." and page 7, paragraph 60, "the markup processor 125 can operate as a security processor to handle security related processing operations on markup language data within messages 140 transferred from the client application 135 to the server application 115");

rewriting any link to a secure webpage such that a request for the secure webpage made by referencing the rewritten link will be recognized by an intermediating device intermediating between a client and a server capable of responding to the request for the secure webpage (page 4, paragraph 27, "URL re-writing" and page 11, paragraphs 96-99, "rewriting URLs in an HTTP header" and "transformation of pre-transform data according to a transformation function");

delivering the scanned webpage to the client (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.");

receiving a request for a secure webpage at the intermediating device, the request based on the rewritten link (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e.

requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.", page 4, paragraph 27, "URL re-writing", page 9, paragraphs 83 and 84 and page 11, paragraphs 96-99, "rewriting URLs in an HTTP header" and "transformation of pre-transform data according to a transformation function");

returning the rewritten link in the request to its original format to thereby accelerate delivery of the requested secure webpage (page 12, paragraph 128);

requesting the secure webpage from the server (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.");

receiving the requested webpage from the server (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.").

15. Regarding claim 18, Kuznetsov teaches establishing a secure connection between the client and the intermediating device (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client

computer system over the computer network for receipt by the client's web browser." and page 7, paragraph 60, "the markup processor 125 can operate as a security processor to handle security related processing operations on markup language data within messages 140 transferred from the client application 135 to the server application 115").

16. Regarding claim 21, Kuznetsov teaches returning the received webpage to the client proxy (page 3, paragraph 25, page 6, paragraphs 56 and 57, page 7 and paragraph 63).

17. Regarding claim 22, Kuznetsov teaches returning the received webpage to the client (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser." and page 7, paragraph 60, "the markup processor 125 can operate as a security processor to handle security related processing operations on markup language data within messages 140 transferred from the client application 135 to the server application 115").

18. Regarding claim 26, Kuznetsov discloses a system for accelerating delivery of requested secure webpages in a network comprising:

a client having first software means for requesting and receiving secure and nonsecure webpages (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and

can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.");

a plurality of servers having second software means for responding to a client's request for secure and nonsecure webpages (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.");

a client proxy having means for rewriting links to any secure webpage in a webpage requested by the client, from an original format of the links such that the client's request for a secure webpage based on a rewritten link will be recognized as a request for a secure webpage by an intermediating device intermediating between the client and the plurality of servers (page 3, paragraph 25, paragraph 27, "URL re-writing", page 6, paragraphs 56 and 57, page 7 and paragraph 63 page 4, and page 11, paragraphs 96-99, "rewriting URLs in an HTTP header" and "transformation of pre-transform data according to a transformation function");

the intermediating device intermediating between the client and the plurality of servers, having third software means for recognizing the rewritten link in a request for a secure webpage, returning the rewritten link to the original format, and using the request with the rewritten link in the original format to obtain the secure webpage from one of the plurality of servers to thereby accelerate delivery of a requested secure webpage (page

1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser." and page 7, paragraph 60, "the markup processor 125 can operate as a security processor to handle security related processing operations on markup language data within messages 140 transferred from the client application 135 to the server application 115").

19. Regarding claim 27, Kuznetsov discloses wherein the client proxy comprises means for delivering a requested webpage to the client (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser." page 3, paragraph 25, page 6, paragraphs 56 and 57 and page 7, paragraphs 60 and 63, "the markup processor 125 can operate as a security processor to handle security related processing operations on markup language data within messages 140 transferred from the client application 135 to the server application 115").

20. Regarding claim 28, Kuznetsov discloses wherein the intermediating device comprises means for delivering a requested webpage to the client proxy (page 3, paragraph 25, page 6, paragraphs 56 and 57, page 7 and paragraph 63).

21. Regarding claim 29, Kuznetsov discloses wherein the client proxy comprises means for scanning any received webpage for any links to a secure webpage (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.", page 4, paragraph 27 and page 7, paragraph 60, "the markup processor 125 can operate as a security processor to handle security related processing operations on markup language data within messages 140 transferred from the client application 135 to the server application 115").

22. Regarding claim 30, Kuznetsov discloses wherein the intermediating device comprises means for setting up a secure connection between the intermediating device and the one of the plurality of servers responding to the request for the secure webpage (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser." and page 7, paragraph 60, "the markup processor 125 can operate as a security processor to handle security related processing operations on markup language data within messages 140 transferred from the client application 135 to the server application 115").

23. Regarding claim 31, Kuznetsov discloses wherein the means for rewriting links to any secure webpage rewrites an https request to be an http request (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.", page 4, paragraph 27, "URL re-writing", page 9, paragraphs 83 and 84 and page 11, paragraphs 96-99, "rewriting URLs in an HTTP header" and "transformation of pre-transform data according to a transformation function").

24. Regarding claim 32, Kuznetsov discloses wherein the means for rewriting links to any secure webpage rewrites the https request to include a reference to a subdomain recognized by the intermediating device to thereby indicate a request for a secure webpage (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.", page 4, paragraph 27, "URL re-writing", page 9, paragraphs 83 and 84 and page 11, paragraphs 96-99, "rewriting URLs in an HTTP header" and "transformation of pre-transform data according to a transformation function").

25. Regarding claim 33, Kuznetsov discloses wherein the client comprises means for establishing a secure connection between the client and the intermediating device

(page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser." and page 7, paragraph 60, "the markup processor 125 can operate as a security processor to handle security related processing operations on markup language data within messages 140 transferred from the client application 135 to the server application 115").

26. Regarding claim 35, Kuznetsov discloses wherein the one of the plurality of servers is a member of a public network (page 6, paragraph 54, "Internet", page 9, paragraphs 84 and 85).

27. (New) Regarding claim 39, Kuznetsov teaches a method to reduce processing requirements on a client requesting secure content from a remote server over the Internet, the method comprising:

identifying a link to a secure webpage received from the remote server by the client (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser." and page 7, paragraph 60, "the markup processor 125 can operate as a security processor to handle security related processing operations on markup language data within messages 140 transferred from the client

application 135 to the server application 115");

rewriting the link to be recognizable by an intermediating device disposed between the client and the remote server (page 3, paragraph 25, paragraph 27, "URL re-writing", page 6, paragraphs 56 and 57, page 7 and paragraph 63 page 4, and page 11, paragraphs 96-99, "rewriting URLs in an HTTP header" and "transformation of pre-transform data according to a transformation function");

enabling the intermediating device to intercept the rewritten link and retrieve the secure webpage (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.", page 4, paragraph 27 and page 7, paragraph 60, "the markup processor 125 can operate as a security processor to handle security related processing operations on markup language data within messages 140 transferred from the client application 135 to the server application 115");

receiving the requested secure webpage from the server onto the intermediating device (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.", page 4, paragraph 27 and page 7, paragraph 60, "the markup processor 125 can operate as a security processor

to handle security related processing operations on markup language data within messages 140 transferred from the client application 135 to the server application 115"); sending the requested secure webpage from the intermediating device to a client proxy (page 3, paragraph 25, page 6, paragraphs 56 and 57, page 7 and paragraph 63).

28. (New) Regarding claim 40, Kuznetsov teaches wherein the step of identifying a link to the secure webpage is selected to be performed by the client proxy (page 3, paragraph 25, page 6, paragraphs 56 and 57, page 7 and paragraph 63).

29. (New) Regarding claim 41, Kuznetsov teaches wherein the step of rewriting the link changes a secure request to a non-secure request (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.").

30. (New) Regarding claim 42, Kuznetsov discloses wherein the step of rewriting the link redirects a secure request to a subdomain (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser." and page 3, paragraph 25, paragraph 27, "URL re-writing", page 6, paragraphs 56 and 57, page 7 and paragraph 63 page 4, and page 11, paragraphs 96-99, "rewriting URLs

in an HTTP header" and "transformation of pre-transform data according to a transformation function").

31. (New) Regarding claim 43, Kuznetsov discloses a processor-readable storage medium storing an instruction that, when executed by a processor, causes the processor to perform a method to reduce processing requirements on a client requesting secure content from a remote server over the Internet, the method comprising:

identifying a link to a secure webpage received from the remote server by the client (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser." and page 7, paragraph 60, "the markup processor 125 can operate as a security processor to handle security related processing operations on markup language data within messages 140 transferred from the client application 135 to the server application 115");

rewriting the link to be recognizable by an intermediating device disposed between the client and the remote server (page 3, paragraph 25, paragraph 27, "URL re-writing", page 6, paragraphs 56 and 57, page 7 and paragraph 63 page 4, and page 11, paragraphs 96-99, "rewriting URLs in an HTTP header" and "transformation of pre-transform data according to a transformation function");

enabling the intermediating device to intercept the rewritten link and

retrieve the secure webpage (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.", page 4, paragraph 27 and page 7, paragraph 60, "the markup processor 125 can operate as a security processor to handle security related processing operations on markup language data within messages 140 transferred from the client application 135 to the server application 115");

receiving the requested secure webpage from the server onto the intermediating device (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.", page 4, paragraph 27 and page 7, paragraph 60, "the markup processor 125 can operate as a security processor to handle security related processing operations on markup language data within messages 140 transferred from the client application 135 to the server application 115");

sending the requested secure webpage from the intermediating device to a client proxy (page 3, paragraph 25, page 6, paragraphs 56 and 57, page 7 and paragraph 63).

32. (New) Regarding claim 44, Kuznetsov discloses wherein the step of identifying a link to the secure webpage is selected to be performed by the client proxy (page 3, paragraph 25, page 6, paragraphs 56 and 57, page 7 and paragraph 63).

33. (New) Regarding claim 45, Kuznetsov discloses wherein the step of rewriting the link changes a secure request to a non-secure request (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.").

34. (New) Regarding claim 46, Kuznetsov discloses wherein the step of rewriting the link redirects a secure request to a subdomain (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser." and page 3, paragraph 25, paragraph 27, "URL re-writing", page 6, paragraphs 56 and 57, page 7 and paragraph 63 page 4, and page 11, paragraphs 96-99, "rewriting URLs in an HTTP header" and "transformation of pre-transform data according to a transformation function").

35. (New) Regarding claim 47, Kuznetsov discloses a system for accelerating delivery of secure socket layer webpages comprising,

a client web page browser installed in a computer operating in a network

environment (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.", page 4, paragraph 27 and page 7, paragraph 60, "the markup processor 125 can operate as a security processor to handle security related processing operations on markup language data within messages 140 transferred from the client application 135 to the server application 115"),

an intermediating server in the network environment addressable by the client web page browser (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.", page 4, paragraph 27 and page 7, paragraph 60, "the markup processor 125 can operate as a security processor to handle security related processing operations on markup language data within messages 140 transferred from the client application 135 to the server application 115"),

a secure webpage server in the network environment addressable by the client web page browser in a manner requesting a secure connection (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to

the requesting client computer system over the computer network for receipt by the client's web browser.", page 4, paragraph 27 and page 7, paragraph 60, "the markup processor 125 *can operate as a security processor to handle security related processing operations on markup language data within messages 140 transferred from the client application 135 to the server application 115*"),

a client proxy associated with the web page browser having software means for rewriting a first format address link to the secure webpage server requesting a secure webpage to a second format addressed to the intermediating server, the intermediating server having software means for rewriting the second format back to the first format for requesting and obtaining said secure web page from the secure webpage server via a secure connection, the intermediating server having software means for redelivery of said secure webpage to the client proxy and the client web page browser, whereby obtaining of secure webpages by the client web page browser from the secure webpage server is initially between the intermediating server and the secure webpage server and then between the intermediating server and the client web page browser (page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser." and page 3, paragraph 25, paragraph 27, "URL re-writing", page 6, paragraphs 56 and 57, page 7 and paragraph 63 page 4, and page 11, paragraphs

96-99, "rewriting URLs in an HTTP header" and "transformation of pre-transform data according to a transformation function").

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 34 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kuznetsov as applied to claim 26 above, and further in view of United States Patent No. 7,181412 to Fulgoni et al., hereinafter Fulgoni.

Kuznetsov significantly discloses the claimed invention as applied to claim 26 above. However, Kuznetsov fails to disclose the limitation found within claims 34, "wherein the client and the intermediating device are members of a private network". Fulgoni discloses this claim limitation, as cited below.

36. Regarding claim 34, Fulgoni discloses wherein the client and the intermediating device are members of a private network (column 5, lines 27-40 and column 6, lines 10-22).

37. The motivation to combine would be to provide an "intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service" (*Fulgoni* – column 6, lines 38-45).

38. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Fulgoni within the methods and apparatus of Kuznetsov in order that "requests for data from one computer to another computer within the same assigned set of IP addresses are considered secure, because the request and the data sent in reply do not get passed to any computer not assigned an IP address within the set" (*Fulgoni* – column 7, lines 6-17).

39. Kuznetsov significantly discloses the claimed invention as applied to claim 26 above. However, Kuznetsov fails to disclose the limitation found within claim 38, "wherein the client proxy comprises means for decompressing the webpage". Fulgoni discloses this claim limitation, as cited below.

40. Regarding claim 38, Fulgoni discloses wherein the client proxy comprises means for decompressing the webpage (column 10, lines 46-67 and column 11, lines 1-22).

41. The motivation to combine would be so that "the internet consumer receives the benefit of faster net data transmission without the need to intervene in the process of decompressing the data with a separate decompression application or tool" (*Fulgoni* – column 11, lines 9-15).

42. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Fulgoni within the methods and apparatus of Kuznetsov "so that the browser application running on PC 12 includes logic to automatically decompress data which has been compressed according to that algorithm" (*Fugloni* – column 11, lines 15-22).

Response to Arguments

43. Applicant's arguments filed 5/19/08 have been fully considered but they are not persuasive.

44. The limitations found within independent claims 1, 14 and 26 are broadly interpreted by the Examiner to be disclosed by Kuznetsov, as cited above pertaining to the rewriting of links and the reception of a webpage, in particular but not limited to page 1, paragraph 11, "A web server software application operating in the web server computer system can receive and process an HTTP web page request and can return or 'serve' a corresponding web page document or file (i.e. requested) in the client request back to the requesting client computer system over the computer network for receipt by the client's web browser.", page 4, paragraph 27, "URL re-writing" and page 11, paragraphs 96-99, "rewriting URLs in an HTTP header" and "transformation of pre-transform data according to a transformation function".

45. The Applicant's limitation of "rewriting, with a client proxy, original format links in first webpages identifying secure webpages" is broadly interpreted by the Examiner to be disclosed by Kuznetsov's disclosure of "URL re-writing" and the "transformation of pre-transform data".

Conclusion

46. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

47. The following United States Patents and Patent Application Publications are cited to further show the state of the art with respect to the secure and successful routing of electronic information, such as:

United States Patent No. 7,181,438 to Szabo, which is cited to show a database access system.

United States Patent Application Publication No. US 2004/0015715 to Brown, which is cited to show systems and methods of placing user identification in the header of data packets.

United States Patent Application No. US 2003/0120593 to Bansal et al., which is cited to show a method and system for delivering multiple services electronically to customers via a centralized portal.

United States Patent No. 7,039,671 to Cullen, which is cited to show dynamically routing messages between software application programs.

United States Patent Application Publication No. US 2003/0200175 to Wang et al., which is cited to show a system and method for evaluating and enhancing source anonymity for encrypted web traffic.

United States Patent Application Publication No. US 2003/0065763 to Swildens et al., which is cited to show a method for determining metrics of a content delivery and global traffic management network.

United States Patent No. 6,484,143 to Swildens et al., which is cited to show a user device and system for traffic management and content distribution over a wide area network.

United States Patent No. 7,272,639 to Levergood et al., which is cited to show internet server access control and monitoring systems.

48. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEREMIAH AVERY whose telephone number is (571)272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

49. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jeremiah Avery/
Examiner, Art Unit 2131

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2131